Overview of France's Intelligence Legal Framework

Félix Tréguer

Overview of France's Intelligence Legal Framework

Félix Tréguer*

December 2021

The Intelligence Act of 24 July 2015 (*loi relative au renseignement*) is a statute adopted by the French Parliament. The law created a new chapter in the Code of Internal Security aimed at regulating the surveillance programs of French intelligence agencies, in particular those of the DGSI (domestic intelligence) and the DGSE (foreign intelligence).

1. Background

The Intelligence Bill was introduced to the Parliament on 19 March 2015 by French Prime Minister Manuel Valls (Socialist Party) and presented as the government's reaction to the Charlie Hebdo shootings. Despite widespread mobilisation, the Bill was adopted with 438 votes in favor, 86 against and 42 abstentions at the National Assembly and 252 for, 67 against and 26 abstentions at the Senate. It was made into law on 24 July 2015.

Although framed by the government as a response to the Paris attacks of January 2015, the passage of the Intelligence Act has a much longer history. The previous law providing a framework for the surveillance programs of French intelligence agencies was the Wiretapping Act of 1991, aimed at regulating telephone wiretaps. Many surveillance programs developed in the 2000s –especially to monitor Internet communications—were rolled out outside of any legal framework. As early as 2008, the French government's White Paper of Defence and National Security stressed that "intelligence activities do not have the benefit of a clear and sufficient legal framework,"

*Félix Tréguer is associate researcher at the CNRS Center for Internet and Society and postdoctoral fellow at CERI-Sciences Po. His research blends political history and theory, law as well as media and technology studies to look at the political history of the Internet and computing, power practices like surveillance and censorship, the algorithmic governmentality of the public sphere, and more broadly the digital transformation of the state and of the security field. He is a founding member of La Quadrature du Net, a French advocacy group dedicated to the defence of civil rights in relation to digital technologies. Contact: felix.treguer@sciencespo.fr – CERI 56 rue Jacob – 75006 Paris FRANCE. Acknowledgement: This research was supported by the French National Research Agency (ANR) through the GUARDINT project (Grant n°18-ORAR-0006-01). felix.treguer@sciencespo.fr.

and said that "legislative adjustments" were necessary. A first and partial attempt at legalisation went underway right after the first Snowden disclosures, with the adoption of the 2013 Military Planning Act in the Fall of 2013[1].

Since it was first adopted, the 2015 Intelligence Act has been amended several time, either in response to new case-law by French and supranational courts, in order to clarify specific provisions whose interpretations had led to controversies within the world of intelligence, and/or to expand intelligence agencies' capabilities. The most significant revision came about in July 2021[2].

2. General provisions

Compared to the 1991 Wiretapping Act (the previous statute in the field of secret sate surveillance), the 2015 Intelligence Act enacts an unprecedented extension of the scope of so-called "intelligence-gathering techniques" (see below).

2.1. Purpose of intelligence

Through article L. 811-3,[3] it also extends the number of objectives that can justify extra-judicial surveillance. These include:

- national independence, territorial integrity and national defence;
- major interests in foreign policy, implementation of European and international obligations of France and prevention of all forms of foreign interference;
- major economic, industrial and scientific interests of France;
- prevention of terrorism;
- prevention of: a) attacks on the republican nature of institutions; b) actions towards continuation or reconstitution of groups disbanded under Article L. 212-1; c) collective violence likely to cause serious harm to public peace;

[1] Tréguer, Félix. 2016. 'From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France'. https://halshs.archives-ouvertes.fr/halshs-01306332/document (July 1, 2016).

[2] See *Loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement*. Codified in the Code of Internal Security, Book VIII "On Intelligence" (article L. 801-L. 898-1).

[3] Unless stated otherwise, all articles mentioned here are part of the Code of Internal Security.

- prevention of organised crime and delinquency;
- prevention of proliferation of weapons of mass destruction.

The government is allowed to extend by decree the number of law enforcement agencies who may conduct extra-judicial surveillance.[4] Finally, any telecom operator or hosting providers failing to comply with the data requests or other surveillance measures can be punished by a two-year imprisonment term and a €150,000 fine (article L. 881-2).

2.2. Oversight

The existing oversight commission, the CNCIS (established in 1991), is replaced by a new Commission called the "National Oversight Commission for Intelligence-Gathering Techniques" (*Commission nationale de contrôle des techniques de renseignement*, or CNCTR). According to the final version of the Intelligence Act –and much like the CNCIS it is comprised of nine members:

- four MPs designated by the Presidents of the Presidents of both chambers of Parliament;[5]
- two administrative judges and two judicial judges designated respectively by the Council of State and the *Cour de Cassation*;
- one technical expert designated by the telecom National Regulatory Authority (the addition of a commissioner with technical expertise was the main innovation).

The commissioners as well as their staff enjoy the highest security clearances so as to perform their duties.

Against previous proposals of an oversight body with extended powers over intelligence agencies, the role of the CNCTR is restricted to the oversight of surveillance measures. The Commission has 24 hours to issue its

[4]Beyond the intelligence community, the *décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure* opened the use of the surveillance techniques listed in the Intelligence Act to dozens of other agencies. The combined staff of these "second circle" agencies is over 45 000.

[5]Interestingly, the 2014 DPR report advocated against the inclusion of MPs in the new oversight body, in light of the increased parliamentary control of intelligence services achieved in recent years through the DPR.

ex ante non-binding opinion regarding the surveillance authorisations delivered by the Prime Minister before surveillance begins,[6] except in cases of "absolute emergency" where it is simply notified of the surveillance measure within 24 hours upon deliverance (article L. 821-3).

As for *ex post* oversight, the CNCTR is supposed to have "permanent, comprehensive and direct access to records, logs, collected intelligence, transcripts and extractions" of collected data. Six years after the adoption of the Act, the tracability of collected intelligence is reportedly unsufficient. According to the DPR:

> The main room for improvement today seems to lie in the still very uneven development, according to the services, of systems for tracing consultations, transcriptions and data extractions, which undeniably weighs on the CNCTR's capacity to conduct a complete and effective control."[7]

The CNCTR is able to conduct visits, both planned and unforeseen, in the premises where these documents are centralised (article L. 833-2-2). If a irregularity is found, it can send to the Prime Minister a "recommendation" so that it can put an end to it. One hugely significant exception to the CNCTR's oversight powers are the bulk of data obtained or sent through data-sharing with foreign intelligence agencies (see blow).

Other bodies form part of the oversight structure for French intelligence:

- In the Fall of 2007, the government of President Nicolas Sarkozy introduced a bill establishing the "Parliamentary Delegation for Intelligence" (*Délégation parlementaire au renseignement*, or DPR), an eight-member strong bipartisan parliamentary committee charged with "keeping track (*suivi*) of the general activity and means" of intelligence agencies.[8] This was a tepid move, but nevertheless amounted to significant change: For the first time, the executive branch conceded to the legislative branch –which is structurally weak under the political regime of the Fifth Republic– some degree of first-hand knowledge of

[6]The non-binding nature of the CNCTR's *ex ante* oversight was criticised by the Bill's opponents. But as the 2014 DPR report had stressed a few weeks earlier, Urvoas and the government recalled that this was necessary to respect the Constitution's article 20 . According to the later, the government "shall have at its disposal the civil service and the armed forces." Since the CNCTR is organically part of the executive branch, the Prime Minister –as head of the government– supposedly cannot be bound by its decisions.

[7]Report on the activity of the Parliamentary Delegation for Intelligence for the year 2019-2021 (June 2020), p. 61. Available at: https://data.guardint.org/en/entity/5fhfis4apmg?searchTerm=marge%20de%20progression&page=61

[8]See *Loi n° 2007-1443 du 9 octobre 2007*. It was not until 2013, however, that the law was amended to substitute the word "*contrôle*" to that of "*suivi*," thereby recognising the delegation's oversight function

what was until then a "*chasse gardée*"[9].

- Inspired by the U.S. style of intelligence governance, several reforms also aimed at strengthening the "*présidentialisation*" of intelligence policy. In 2008, the Élysée created the office of National Intelligence Coordinator as well as the National Intelligence Council. At least on paper (because the President already had de facto authority on the DGSE), the reform undermined the Prime Minister's authority over intelligence agencies.

3. "Intelligence-gathering techniques"

The Intelligence Act lists various procedures for the collection of communications intelligence.

3.1. Wiretaps and access to metadata

Techniques of communications surveillance include telephone or Internet wiretaps (L. 852-1), surveillance of open WiFi networks (L. 852-2), the use of IMSI-Catchers (L. 851-6), satellite interceptions (L. 852-3), access to identifying data and other metadata (L. 851-1), geotagging (L. 851-4) and computer network exploitation (L. 853-2), all of which are subject to authorisation of a (renewable) duration of four months. The Acts also legalises the use of GPS-Tracking devices (L. 851-5) as well as covert listening devices in private premises (L.853-1).

3.2. Automated and real-time analysis of metadata

The Act authorises the use of scanning device (nicknamed "black boxes" by a government adviser in March 2015) to be installed on the infrastructures of telecom operators and hosting providers to analyse in real-time telephone or Internet metadata. Black boxes are authorised after an opinion by the CNCTR, for a duration of two months. Article L. 851-3 of the Code of Internal Security provides that,

> for the sole purpose of preventing terrorism, automated processing techniques may be imposed on the networks of [telecom operators and hosting providers] in order to detect, according to

[9]See Laurent, Sébastien Yves. 2015. 'Le Contrôle Parlementaire Du Renseignement (1971-2015) : Les Enjeux Politiques d'une Tardive Banalisation'. In *Mélanges En l'honneur de Bernard Lachaise*, Riveneuve, 372–96..

> selectors specified in the authorisation, communications that are likely to reveal a terrorist threat.[10]

This provision led to much discussions during parliamentary debates. The Minister of Defence, Jean-Yves Le Drian, explained that the goal was to detect "connections a certain hours, from certain places, on certain websites." In that case, the operational goal is to detect the IP addresses or telephone numbers of known terrorist suspects with potential recruits, or to spot those who try to connect to a "terrorist website." The Director of the DGSE, Bernard Bajolet, gave another example during a committee hearing, asserting that the goal was to "discern clandestine attitudes," alluding to the use of cryptographic and anonymizing tools (for instance using a proxy server).

As for the exact technical nature of these real-time traffic-scanning devices, critics of the proposal feared that the government would use potentially extremely intrusive technologies known as "Deep Packet Inspection" (DPI), which would enable the automatic analysis of all communications flowing through the network.[11] The government –this time through Interior Minister Bernard Cazeneuve, who complained about the "prevailing hubbub and media uproar"– said it would not use DPI.

It took the government until 2017 to roll-out the first of these devices. In mid-2021, when the sunset clause under which this provision was adopted finally came to end after being extended, the government submitted a report to the Parliament asserting that it had made a very limited use of the provision (according to the CNIL, the French data protection authority, only two or three of these black boxes have been deployed since 2017, and only for telephone metadata[12]). This limited use is apparently the consequence of a strong disagreement between the government and the CNCTR on the definition of metadata: whereas intelligence officials sought to scan URLs beyond mere domain names, the CNCTR opposed this move, citing constitutional case-law limiting the surveillance of communications content. To overcome this stalemate, the 2021 reform explicitly expanded the provision to cover detailed URLs.

While the specifications were never made explicit in the 2021 reform bill, the government indicated to the CNCTR and to the CNIL that for

[10] Full sentence in French: "*il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste.*"

[11] Deep Packet Inspection a form of computer network packet filtering that examines the data part (content) –and possibly also the header (or metadata)– of a packet as it passes an inspection point (source: Wikipedia).

[12] See *Déliberation n° 2021-040 du 8 avril 2021 portant avis sur les articles 11 quinquies sexies et septies du projet de loi relatif a la prévention d'actes de terrorisme et au renseignement.*

technical reasons, rather than installing these black boxes on the infrastructure of technical intermediaries as it was the case since the 2015 reform, the later would be asked to copy their metadata traffic in bulk and send it to the Prime Minister's technical office task with implementing intelligence surveillance measures, the GIC (*Groupement interministériel de contrôle*), where it would be stored for 24 hours and scanned[13]. The CNIL expressed serious concerns and said that such an infrastructure of surveillance should be spelled out in the statute considering that it entailed an even more serious interference in the right to privacy.

Even prior to these contentious changes, the provision appeared in breach of EU law. According to the *La Quadrature du Net* ruling of October 6$^{\text{th}}$, 2020:

> the interference resulting from the automated analysis of traffic and location data, such as that at issue in the main proceedings, is particularly serious since it covers, generally and indiscriminately, the data of persons using electronic communication systems. That finding is all the more justified given that, as is clear from the national legislation at issue (...), the data that is the subject of the automated analysis is likely to reveal the nature of the information consulted online. In addition, such automated analysis is applied generally to all persons who use electronic communication systems and, consequently, applies also to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with terrorist activities."[14]

With this ruling, the Court indicated that this "particularly serious interference" could only meet the requirement of proportionality "only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary." Finally, the Court stressed that the implementation of such automated surveillance of metadata must be "be subject to effective review, either by a court or by an independent administrative body whose decision is binding."

Now, current French law does not seem to abide by any of these standards. Article L851-3 of the Internal Security Code authorises this measure in a general way and as a matter of principle, without being conditioned to any "genuine and present" threat (in its ruling of April 21$^{\text{st}}$, 2021, the Council of State chose to shelter French law from the CJEU ruling by alleging that France was under a near-perpetual threat against its national

[13] *Ibid.* (§ 14 to 18).

[14] CJEU, *La Quadrature du Net and Others v Premier Ministre and Others*, §172-182.

security.[15] French law does not provide a framework for this measure within a "strictly limited period" and in practice these devices have been authorised without interruption for the past four years. Lastly, authorisations to engage in such automated and real-time surveillance are subject to an *ex ante* opinion of the CNCTR, which by law is not binding (according to the CNCTR however, its opinions have never disregarded by the Government since the adoption of the Intelligence Act in 2015).

Another provision limited to anti-terrorism allows for the real-time collection of metadata (article L. 851-3, for terrorism only and for a 4 months period). Initially, the provision targeted only individuals "identified as a [terrorist] threat." After the 2016 Nice Attack, it was extended by a Bill of the state of emergency to cover individuals "likely to be related to a threat" or who simply belong to "the entourage" of individuals "likely related to a threat". According to La Quadrature du Net, this means that the provision can now potentially cover "hundreds or even thousands of persons (...) rather than just the 11 700 individuals" reported to be on the French terrorism watchlist." Following a decision by the Constitutional Council in response to a legal challenge introduced by La Quadrature du Net[16], a quota similar to those already in place for wiretaps were introduced to cap the maximum number of authorisations that can be valid at any given time (with a maximum of 720 simultaneous authorisations as of 2020).

3.3. Computer Network Exploitation

The Act authorises hacking as a method for intelligence gathering. Article L. 853-2 allows for:

- access, collection, retention and transmission of computer data stored in a computer system;
- access, collection, retention and transmission of computer data, as it is displayed on a user's computer screen, as it is entered by keystrokes, or as received and transmitted by audiovisual peripheral devices.

Considering the intrusiveness of computer hacking, the law provides that these techniques are authorised for a duration of thirty days, and only "when intelligence cannot be collected by any other legally authorised mean." The data thus obtained can be stored for up to two months after collection[17].

[15] To comply with the CJEU however, the Council of State forced the government to "declare" such threats on national security every year with the adoption of an *ad hoc* executive decree.Conseil d'État, arrêt n°393099 du 21 avril 2021 (FDN et autres) *(§44-46).*

[16] *Décision n° 2017-648 QPC du 4 août 2017.*

[17] The maximum duration for the retention of this data was originally one month. It was doubled by the reform of 2021, without the government providing information as to why such extension was necessary.

The Act also grants blanket immunity to intelligence officers who carry on computer crimes into computer systems located abroad (article 323-8 of the Penal Code). This, in turn, may contravene article 32(b) of the Budapest Convention on Cybercrime on the trans-border access to computer data.[18]

3.4. Forced cooperation of private actors for bulk hacking

Although neither the explanatory memorandum nor the impact assessment carried out by the government mentioned it, article 12 of the 2021 reform made a few changes to the provisions listing the obligations of telecom operators. These changes were nevertheless addressed by Gérald Darmanin, minister of the Interior, when he explained on public radio that in order to circumvent the encryption of communications, "we are discussing with the major Internet companies, we are asking them to let us in via security holes, some accept it, others do not. We probably need a law to constrain foreign services, it is coming."[19]

Article 12, which amended article L. 871-6 of the Code of Internal Security, seems to allow intelligence agencies to compel operators and providers of electronic communications (such as Orange, SFR, but also Whatsapp or Signal according to EU law) to assist in the deployment of vulnerabilities on the terminals of targeted persons. This interpretation was confirmed by one of the bill's rapporteurs, and during subsequent Parliamentary debates. The Interior Minister then answered a question by a minority member of Parliament on the issue:

> As for encrypted messengers, such as Telegram, WhatsApp or Signal, they have precisely built their economic model on the guarantee of not being able to be listened to. Let's be clear: it's not about listening in on phone conversations that take place on these applications, but about taking advantage of the fact that they pass through internet connections. For the most dangerous targets, and under the control of the CNCTR, the collection of computer data will allow access to the computer terminal of the person who uses these messaging systems to collect the data that are stored in these messaging systems.

To illustrate this point, the minister explicitly referred to the Encrochat operation conducted in 2020, in which led the French police deployed a

[18] *T-CY Guidance Note #3 Transborder access to data (Article 32)* (T-CY (2013)7 E). (2014). Council of Europe. https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V11.pdf

[19] France Inter, "Gérald Darmanin : face au terrorisme, 'il ne faut être ni résigné ni outrancier"'. Available at: https://www.franceinter.fr/emissions/l-invite-de-8h20-le-grand-entretien/l-invite-de-8h20-le-grand-entretien-28-avril-2021

particularly complex computer attack involving the exploitation of vulnerabilities to get access to hack the devices of thousands of phones at the same time[20].

3.5. Foreign surveillance

The Act also legalises the DGSE's bulk surveillance apparatus developed since 2008 under a chapter on the "surveillance of international communications." International communications are defined as "communications emitted from or received abroad," that is to say, to put it more simply, going in or out of the country.

The legal regime created here is a complex one:

- For the collection of "international communications," the Prime Minister "designates" (rather than "authorises") which network infrastructure (e.g. the cable-landing stations owned by telecom operators) are subject to large-scale interception (article L. 854-2-I).

- After collection, "when it appears" that both ends of the communications are coming from "technical identifiers that are traceable to the national territory" (e.g.: emitter and receiver are using French telephone numbers or IP addresses), article L. 854-1 provides that intercepted communications "shall be immediately deleted," unless the persons targeted are physically located abroad and either i) already covered by a national surveillance authorisation or are ii) deemed to be a national security threat. However, given the transnational nature of Internet communications, and the fact that a communication between two French residents is likely to be routed in and out of French borders, one can doubt on the effectiveness of such a safeguard.

- For bulk analysis of intercepted metadata (what the Act calls "non-individualised *exploitation*" of metadata), the Prime Minister issues an one-year authorisation specifying the purposes of such analysis and which intelligence agencies are in charge of conducting it (article L. 854-2-II). This seems to refer to the automated-scanning of intercepted metadata, similar to black boxes, but this time not restricted to anti-terrorism.

- For the exploitation of the *content* of communications or of their metadata, the Prime Minister issues a four-month authorisation specifying the purposes justifying such analysis, the intelligence agencies in

[20] Goodwin, B. (June 21, 2021). *Secrecy around EncroChat cryptophone hack breaches French constitution, court hears.* ComputerWeekly.com. Available at: https://www.computerweekly.com/news/252501921/Secrecy-around-EncroChat-cryptophone-hack-breaches-French-constitution-court-hears

charge, as well as targeted geographic zones, organisations, groups of people or individuals.

Originally, the CNCTR was only notified of all authorisations related to international surveillance and can issue recommendations to the Prime Minister if irregularities were found. However, a few months after the adoption of the 2015 Intelligence Act and at the request of the Prime Minister, the CNCTR agreed to conduct such *ex ante* oversight on an experimental basis by issuing prior opinions over requests for the exploitation of intercepted communications provided for in section III of Article L. 854-2. This extension of the CNCTR's oversight powers has been effective since the end of May 2016. In 2018, the law was amended to provide a legal basis for this *ex ante* oversight[21]. In breach of European law, French law does not provide any redress mechanisms for foreigners (including people living in other EU Member States) that might be subject to international surveillance measures.

3.6. Data retention periods

For national surveillance measures, once communications data are collected by intelligence agencies, retention periods are the following:

- Content (*correspondances*): 1 month after collection (for encrypted content, period starts after decryption, within the limit of 6 years after initial collection);
- Metadata: 4 years (compared to the LPM decree 3-year period).

For international surveillance, retention periods depend on whether one end of the communication uses a "technical identifiers traceable to the national territory" or not, in which case the "national" retention periods are applicable, but they start after the first exploitation and no later than six months after collection (article L. 854-8). If both ends of the communication are foreign, the following periods apply:

- Content: 1 year after first exploitation, within the limit of 4 years after collection (for encrypted content, periods starts after decryption, within the limit of 8 years after collection);
- Metadata: 6 years.

[21] See *loi n°2018-607 du 13 juillet 2018*, article 37.

3.7. Data-sharing between French intelligence agencies

The 2018 reform amended the provisions regarding international surveillance in order to facilitate the use DGSE's data by domestic intelligence for French residents – surveillance activities that the original 2015 Act had sought to restrict[22]. As Florence Parly, then minister of Armed Forces, explained upon introducing the amendment; "First, we want to allow the exploitation of data of a technical identifier traceable to the national territory intercepted in the context of the surveillance of international communications, even though its user is in France."

Article L. 854-2 V thus provides a new type of surveillance technique, where the Prime Minister allows – after an opinion by the CNCTR – for the exploitation of the content of communications and/or metadata collected through international surveillance of a person currently in France – something that the 2015 Intelligence Act had explicitly ruled out. The same provision also provides that wiretaps and metadata surveillance authorisations issued in the context of domestic intelligence (articles L. 851-1,L. 851-2 and L. 852-1 I) can also encompass the exploitation of data collected and stored under the international surveillance regime.

Secondly, the government sought to authorise surveillance operations known as "doubt removal". According to the minister of Armed Forces:

> The removal of doubt will take the form of a spot check on metadata legally intercepted in the context of international communications surveillance. These are very quick operations, ones that not repeated and are likely to reveal a relationship graph or the presence of a person abroad, who could then be monitored if he or she presents a threat. As soon as the verification reveals the need for surveillance, the exploitation of communications can only be pursued via the intelligence techniques enshrined in the 2015 law."[23]

Through this new provision, intelligence analysts are able to use one or more "selectors" or "identifiers" corresponding to persons or groups of persons located abroad to probe databases for French-related metadata. By doing so, they can build the target's social graph and identify other potential suspects currently in France. These suspects' communications can then be further monitored under the national surveillance regime (e.g., by requesting authorisation to conduct a security interception). In the case of a "urgent" terrorist threat or national cybersecurity threat, "doubt removal" queries can exceptionally be conducted with French technical identifiers and cover

[22] On this legislative change, see also CNCTR's 2018 Annual Report, p. 28.

[23] See the minutes of the Senate session where the amendment was introduced, May 22, 2018. www.senat.fr/seances/s201805/s20180522/s20180522022.html

not only metadata but also the content of communication. In such case, it becomes possible to retrace the history of a French resident's communications by going back six years in the past (data retention period provided for in the "international surveillance" regime), whereas the national surveillance regime allowed for the collection of metadata from operators and a number of hosting companies that were no more than one year old.

Beyond the special case of international surveillance and the use of data collected under this regime by domestic intelligence, French intelligence agencies can share data and intelligence. The original drafting of the 2015 Intelligence Act did not provide any strong safeguards for such data sharing, as the government declined for years to adopt an implementation decree. In April 2019, *Le Monde* revealed that a data warehouse (an infrastructure nicknamed "*entrepôt*") had been built next to the DGSE facilities to provide a kind of "fusion center" to French intelligence agencies[24]. Finally, with the threat of litigation rising, the 2021 reform bill established a more detailed legal regime for these activites. Article L. 822-3 now provides that collected data and associated intelligence can be shared with another agencies. Such data sharing is subject to a authorisation of the Prime Minister and a prior opinion of the CNCTR if i) the data is shared for different purposes than those that justified the original authorisation (e.g. ancillary use of data for counter-espionage purposes when the data was first collected for the purpose of fighting terrorism) or ii) when the intelligence agency with which the data is shared has no prerogative over the matter for which collection was first authorised.

Lastly, article L. 863-2 of the Code of Internal Security provides that intelligence services may require any data, including personal data (with the exception of genetic data) to other public bodies.

3.8. Experimentation and research

In 2018, the French government built on a provision first adopted in 2017 to expand the possibility for agencies part of the Ministry of the Armed Forces to engage in trials of surveillance devices like IMSI catchers or those used for international surveillance and the surveillance of radio communications (article 2371-2 of the Code of Defence). The CNCTR is notified prior to the roll-out of these tests and is informed of their scope.

In 2021, another legislative provision dedicated to research and development was introduced by the government. Next to the DGSE's Big Data tools, French domestic intelligence has also worked with Palantir's technolo-

[24]Follorou, J. (2019, April 24). '« L'entrepôt », bâtiment ultrasécurisé et outil essentiel du renseignement français'. *Le Monde*. https://www.lemonde.fr/societe/article/2019/04/24/l-entrepot-un-outil-essentiel-du-renseignement-qui-fonctionne-sans-cadre-legal_5454225_3224.html

gies from 2016 onwards to mine and analyse collected data[25]. The growing use of Artificial Intelligence techniques led to the adoption of article L. 822-2 III, which provides that collected data can be stored for up to five years and used as training data for "the acquisition of sufficient knowledge to develop, improve and validate the technical capacities of collection and exploitation."

4. Redress mechanism

The Intelligence Act reorganises redress procedures against secret surveillance, establishing – and this is one of the main innovations of the 2015 Act – the possibility to introduce a legal challenge before the Council of State. The procedure is the following:

- Any legal person can introduce a complaint to the CNCTR, asking the oversight body to investigate whether or not she has been subject to illegal surveillance measures (article L. 833-4). The CNCTR can then only notify the plaintiff it has carried on necessary checks, "without confirming or denying" whether or not they have been spied upon.
- Only after taking this preliminary step, plaintiffs can appeal to the Council of State, who is competent in first and last resort. The same procedure is opened to the CNCTR when its investigations uncovered irregularities but only when, once notified by the CNCTR, the Prime Minister has failed to take appropriate action.
- Intelligence-related cases are adjudicated by a new, three-judge special court within the Council of State (so-called "specialised panel" or "specialised court"). The court's judges and their staff have security clearance and can access any piece of information collected by the CNCTR (initial authorisation, collected transcripts, etc.). The Act provides that the right of the defense, and in particular the right to open justice, may be "accommodated" to protect classified information. In practice, much of the evidence presented by the government to justify the necessity and proportionality of the surveillance measure will remain hindered from the plaintiffs and her lawyers (article L. 773-2 of th Code of Administrative Justice).
- When it finds a surveillance operation to be illegal, the specialised court can (but is not obliged to) put an end to it and/or order the collected data to be destroyed (article L. 773-7 of the Code of Administrative Justice). Without compromising state secrets, it can then

[25]'A French Alternative to Palantir Would Take Two Years to Make, Thales CEO Says'. December 8, 2020. *Reuters*. Available at: https://www.reuters.com/article/us-thales-ceo-idUSKBN2782FS.

inform the plaintiff that the government has carried an illegal act, and order the state to pay damages.

This redress procedure seems inspired by the so-called "closed-material procedure" established in the UK through the Justice and Security Act of 2013, which are criticised for their detrimental impact on defence rights.[26] The DPR has also stressed the shortcomings of this reddress mechanism:

> The specialised panel appears unable to ensure, if this were to be raised in the context of litigation, that the intelligence techniques used do not lead to the collection of data other than that for which they were authorised, or that the database relating to state security comply, in their operation and content, with the legal framework and fundamental freedoms. The president of the specialised panel of the Council of State also observed that lawmakers had not adopted any specific provision to guarantee the implementation, by the intelligence agencies, of its rulings regarding intelligence techniques."[27]

5. Major oversight gaps in the French intelligence legal framework

In this last section, we provide an overview of some major oversight gaps in the French legal framework surrounding intelligence.

5.1. International data-sharing

Article L. 833-2-3 explicitly forbids the CNCTR to conduct any form of oversight on data shared with foreign intelligence partners. Following criticisms by civil society organisations during the parliamentary debate in 2015 the CNCTR has voiced in several annual reports an important oversight gap regarding the sharing of data between French intelligence services and foreign services. In France, the issue is all the more pressing because the data flows exchanged between the General Directorate for External Security (DGSE) and the National Security Agency (NSA) have increased rapidly following the conclusion of the SPINS agreements, signed at the end of

[26] Didier Bigo *et al. National Security and Secret Evidence in Legislation and Before theCourts: Exploring the Challenges.* Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs PE 509.991. Brussels: European Parliament, 2014, p. 156.

[27] Report on the activity of the Parliamentary Delegation for Intelligence for the year 2019-2020 (June 11, 2020).

2015 between France and the United States[28]. Yet the 2015 law explicitly excluded any control by the CNCTR over these international collaborations nurtured by networks of intelligence professionals enjoying strong autonomy.

In its annual report published in 2019[29], the CNCTR admitted that this "black hole" in intelligence control presented a major risk, since it could allow French services to receive data from their counterparts that they would not have been able to obtain legally through the procedures provided by French law. The CNCTR considered that "a reflection [should] be carried out on the legal framework for data exchanges between French intelligence services and their foreign partners."

In support of this request, the CNCTR referred to the case law of the European Court of Human Rights (ECHR), which again recalled in its *Big Brother Watch v. United Kingdom* judgment of May 25, 2021 that these exchanges should be governed by national law and subject to the control of an independent authority[30]. According to a report by the Fundamental Rights Agency of the EU, France is currently the last European Union member state to have no legal framework for these international exchanges[31].

5.2. Right to information of persons under surveillance

Another essential principle identified by European case law is the right to information of persons who have been the subject of a surveillance measure, once such information is no longer likely to hinder the investigation conducted against them by intelligence agencies. In a report published in January 2018, the CNCTR reviewed the relevant case law and mentioned several examples of foreign legislation – German law in particular – guaranteeing a procedure for notifying persons under surveillance and providing for a number of narrowly limited exceptions. The CNCTR was forced to note that, as French law stands, "persons under surveillance cannot be informed of the intelligence techniques implemented against them."[32] The 2021 reform bill completely overlooked this issue.

The government has also set aside another requirement, again stressed by the Council of State in its ruling of April 21, 2021 on the indiscriminate retention of metadata. In this decision, which largely won the government's case, the Conseil d'État echoed the CJEU's *La Quadrature du Net*'s ruling

[28]'FR-US Deal Unveiled', June 29, 2016. *Intelligence Online*. https://www.intelligenceonline.com/government-intelligence_organizations/2016/06/29/spins--fr-us-deal-unveiled,108172546-art

[29]See CNCTR Annual Report 2018, p. 50.

[30]ECHR, *Big Brother Watch and others v. United Kingdom* (Grand Chamber Judgment), May, 25 2021, § 362)

[31]Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II: field perspectives and legal update, Fundamental Rights Agency (2017), p. 52. Available at: https://data.guardint.org/en/entity/0t6462gq7i1d?page=52

[32]See CNCTR Annual Report 2017, p. 85-86.

by indicating that the opinions rendered by the CNCTR on surveillance measures should be "binding" rather than merely consultative. In spite of the CNIL's insistence that the 2021 reform bill should address this concern, the government refused to do so.

5.3. Lack of oversight on intelligence databases

As for the joint desire of the DPR and the CNCTR to guarantee the latter a right of review over intelligence databases, it is coming up against the fierce opposition of the services. As parliamentarians from the DPR have emphasised, this is a crucial stage in the oversight process, as it is the only way for the CNCTR to "ensure that no data has been collected, transcribed or extracted in disregard of the legal framework, or even in the absence of an authorisation granted by the Prime Minister."[33] And yet, a person close to the Ministry of the Interior complains about the regulatory burdens. According to them, "the police are required to do crazy things" and "even the smallest pizza vendor can cross-reference more computer data than our intelligence agencies."[34]

5.4. No legal framework for OSINT, infiltration and postal surveillance

The French legal framework around intelligence is completely silent regarding other typical surveillance techniques that are extremely sensitive from the point of view of civil liberties. This is the case of the surveillance of letters and postal packages, or the infiltration of certain groups by intelligence agents. In the United Kingdom, however, the Investigatory Powers Act of 2016 covers these two areas.

The French law also makes no mention of so-called "open source" surveillance, notably on social networks such as Facebook or Twitter – an activity about which little has been leaked to the press but which is known to have grown in importance over the last ten years[35]. The DPR recently confirmed it was the case: "[French] intelligence agencies collect and exploit intelligence of cyber origin from the innumerable sources freely available on the Internet, but also by means of techniques which are subject to a legal framework (...)."[36]

[33]Report on the activity of the Parliamentary Delegation for Intelligence for the year 2019-2020 (June 11, 2020). Available at: https://data.guardint.org/en/entity/5fhfis4apmg?page=100

[34]Quoted in Valdiguié, L. November, 16 2020. 'Le programme "X", un logiciel espion surpuissant pour traquer les terroristes'. https://www.marianne.net/societe/terrorisme/le-programme-x-un-logiciel-espion-surpuissant-pour-traquer-les-terroristes.

[35]*Ibid.*

[36]Report on the activity of the Parliamentary Delegation for Intelligence for the year 2019-2020 (June 11, 2020). Available at:

Still, a high-raking intelligence officials was quoted by a journalist as complaining over the bureaucratic burdens entailed by French law, claiming that "we have the most restrictive regulations in Europe: we have to constantly ask for authorisations from the CNCTR."[37]

5.5. Right to information and whistleblowing

Apart from the few pieces of information that have filtered through thanks to the small circle of specialised journalists who have access to sources within the services, and apart from the rare allusions made concerning these topics by those in charge of intelligence during parliamentary hearings or by the CNCTR, no official information is provided on the nature of the technologies used by the services and their imbrication in the processes of production of intelligence, on the public contracts and the identity of the private subcontractors, nor even on the legal interpretations that are used within the services.

Here again, the comparison with the main European intelligence powers reveals the French democratic delay. To be convinced of this, one simply has to consult the report published in August 2016 by David Anderson in the margin of the parliamentary debate on the Investigatory Powers Act[38]. This jurist in charge of the independent monitoring of anti-terrorism legislation reported on the technological capacities for "bulk powers" data collection and exploitation. He also gave several examples of use cases in which these technologies were employed and evaluated their operational interest based on internal documents and interviews with certain senior officials.

In France, such a degree of transparency seems unimaginable for the moment. Even if the CNCTR has made some progress in the precision of the information provided in its reports, it is essentially content to describe the state of the law and its evolution, or to disseminate general statistics on the types of measures authorised and their purposes. This is still far from the level of detail that feeds the public debate and the work of parliamentarians, journalists or NGOs in countries such as the United Kingdom or Germany.

Finally, following a recommendation of the Council of State in its 2014 report, Urvoas, the 2015 Intelligence Bill rapporteur at the National Assembly, passed an amendment turning the CNCTR into an internal whistle-blowing channel for intelligence officers. But the provision remains very limited in scope.[39]

---

https://data.guardint.org/en/entity/5fhfis4apmg?page=266

[37] *Ibid.*

[38] Anderson, D. Report of the Bulk Powers Review. *Independent Reviewer of Terrorism Legislation* (August 2016).

[39] The range of abuses that can be reported are limited to criminal violations of the confidentiality of communications. Cases of active corruption, for instance, are not covered. What is more, a last-minute governmental amendment deleted the sentence granting po-

Moreover, the Act increases the criminal repression of disclosures regarding the "existence of the deployment" of a given surveillance technique (article L. 881-1): Such unauthorised disclosures are punished by a two-year imprisonment term and a €150 000 fine (against a two-year term and a €30 000 fine before). Lastly, the court rulings of the Council of State's special section and its general case-law will remain secret (article L. 773-7 of the Code of Administrative Justice).

All of these provisions affecting the right to information obviously fail to comply with international best-practices, such as those laid down in the Tshwane principles on national security and the right to information.[40]

tential whistleblowers the right to "testify about classified information, information that might harm the security of personnels, or undermine the missions of intelligence agencies." This creates huge legal insecurity for potential whistleblowers.

[40] *The Global Principles on National Security and the Right to Information (Tshwane Principles).* 2013. Open Justice Initiative. Available at: https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.